# Emerging Technologies and Data Regulatory Frameworks: Implication of AI, Big Data, Blockchain and Biometrics on Data Privacy and Compliance

Muhammad Dini Ibrahim[1], Yahaya Salisu[2], Ibrahim Abdullahi Aliyu[3], Aliyu Ibrahim Sulaiman[4], Abdulrazak Jibril Baba[5], Nuraini Usman[6]

**[1, 2,3,4,5]Department of Computer Science and Engineering, Shobhit University, Meerut, Uttar Pradesh, India.**

**[6]Department of International Programmes, Jigawa State Polytechnic for Information and Communication Technology (JSPICT), Kazaure, Nigeria**

**ABSTRACT**

**The exponential dynamics of Artificial Intelligence (AI), Big Data, Blockchain, Biometrics, and Internet of Things in the name of emerging technologies make it easier for how data is collected, stored, maintained, and processed across organisations, increasing the data ecosystem in the context of volume, velocity, and sensitivity of information exchange. These technologies are rapidly evolving with new opportunities for greater efficiency, accuracy, and transparency. Emerging technologies improve operational efficiencies and enable data-driven innovations, also resulting in simultaneous complex data privacy issues, regulatory compliance, and ethical governance. This paper critically examines the intersection of emerging technologies, data privacy, and regulatory compliance, considering Nigeria's Data Protection Acts (NDPA) 2023, the Indian Digital Personal Data Protection (DPDP) Act, 2023, and global acts like the General Data Protection Regulation (GDPR)-EU. It analyses how these technologies can be effectively implemented by individuals and organisations while maintaining sustainable trust in digital ecosystems, necessitating technical safeguards and integrations. Through implementation, organisations can align technological advancement with global privacy standards, augmenting innovations and mitigating risks in the future. Strategies and recommendations are made to inform policymakers, regulators, and practitioners in the balancing of innovation with strong data privacy protections and compliance.**

***Keywords:*** *Global Data Protection Regulation, Indian Digital Personal Data Protection, Nigeria Data Protection Regulation, Emerging Technologies, Data Privacy*

## 1.0 INTRODUCTION

Based on the technological innovations dynamics, AI, IoT, Big Data, Blockchain, Cloud Computing, and Biometric systems are rapidly transforming the way public and private organisations collect, process, and store their data. These brings sophistication in decision-making and foster innovation methodologies. In Nigeria, public and private organisations are increasingly adopting these technologies to fast-track online presence and deliver digital services to citizens and customers in an efficient and transparent process. The implementation of these technologies comes with a greater concern about data privacy, adaptability, regulatory compliance, and data security. The amount of data generated by AI models, IoT devices, sensors, and biometric systems increases the risks of data breaches, unauthorised access, and misuse of personal data. Meanwhile, governments and institutions around the globe are implementing tougher data privacy and regulatory acts, such as GDPR EU, DPDP Act (India), and the NDPA in Nigeria (Dhirani et al. 2023a; Aloamaka 2023a).

Despite the availability of different acts and frameworks on data protection and regulatory compliance, most organisations struggle to adopt and implement the intersection of technologies and data protection principles. Problems such as a lack of adequate awareness, technical skills, expertise, poor institutional frameworks, and low privacy-by-design practices (Ajayi 2025). These problems are mostly common in developing nations like Nigeria, where digital transformation is high, but data privacy and regulatory compliance are not widely practised and supported.

This paper critically reviews the nexus of emerging technologies and data privacy in Nigeria and global best practices. Hence, we analysed how AI, Big Data, IoT, Cloud Computing, Blockchain, and Biometric systems influence privacy and regulatory compliance requirements and recommend pragmatic strategies for individuals, organisations, and policymakers to effectively balance technological innovation with the protection of individual rights and data privacy.

## 2.0 BACKGROUND AND LITERATURE REVIEW

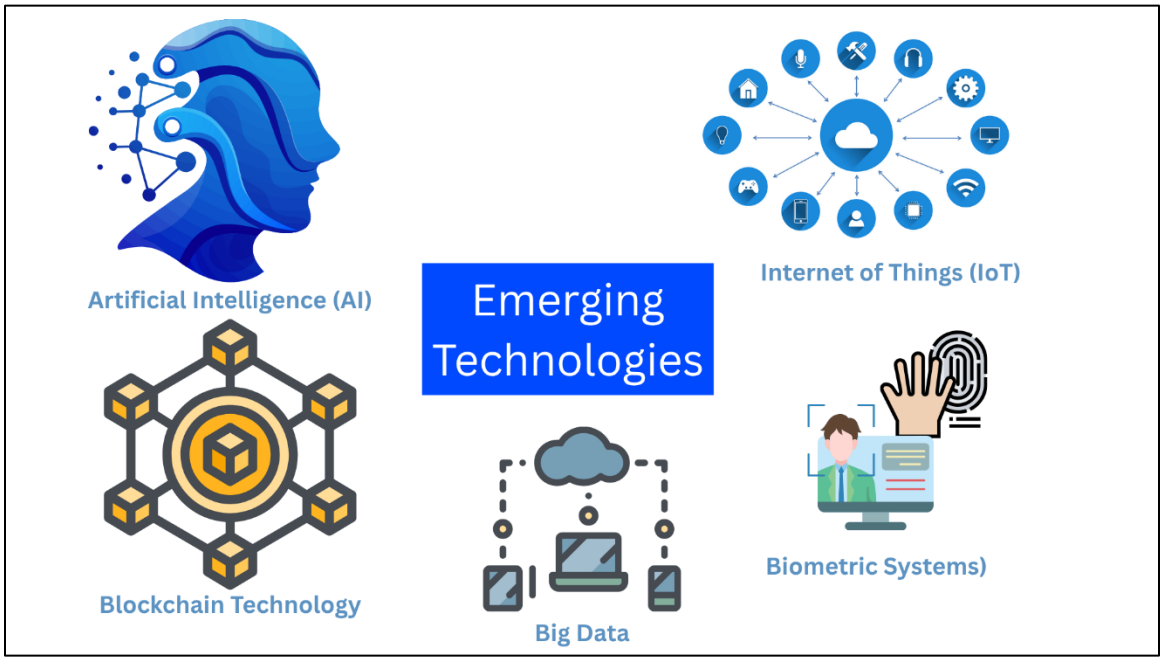
Emerging technologies are the new wave of technological advancement that aim for high precision and efficiency in the delivery of automated services (Dhirani et al. 2023b). This includes AI, Cloud Computing, Autonomous Vehicles, Big Data, Machine Learning (ML), Wearables, Biometrics, and Surveillance Systems. Technology advancements like AI and Extended Reality (XR) integration that incorporate virtual, augmented and mixed reality possess unique and significant risks to users, such as Pervasive Profiling, Membership Inference Attacks (MIA), Model Inversion Attacks (MIA), and Linkage Attacks. This issue originates from broad scope collection of highly sensitive sensor data, XR devices, specifically VR headsets and AR glasses, are furnished with many sensors (e.g., cameras, microphones, eye trackers, motion sensors) capturing biometric and physiological data on a big scale which AI model process and analyse to create a highly defined user profile (Alkaeed et al. 2024).

Big data in sectors such as healthcare, which has volume, velocity, and veracity merged from Electronic Health Records (EHRs), genomic data, and information from wearable/mobile devices**,** also poses significant risks such as re-identification risk, inadequate consent, and inference-based breaches in accordance with (Yuan and Singh, n.d.), Analytics of big data to draw meaningful insights is a paramount achievement; however, it presents considerable privacy risk, especially when there's a lack of good policy governance, some of which has emerged from profiling activities like deanonymisation and linkage attacks. (Tran and Hu 2019). In a gesture of making sure individual users retain the sovereignty over the extensive personal data generated by their connected IoT devices, Personal Data Stores (PDS) are leveraged as a technology that ensures user-centric data governance, allowing discretion on the permissions of access control (Pinto et al. 2024).

Blockchain's immutability to track and record transactions permanently conflicts with the legal right of erasure (or the "right to be forgotten"). Reconciling such technical versus legal impediments requires systems to employ an architectural mitigation pattern where information is classified, user-sensitive personal data is saved off the chain ledger, and

pointers are used to link with the unclassified sensitive part of the information. (Zafar 2025). Building upon this finding (Zafar 2025), further demonstrates deployment of blockchain to manage personal data introduces risks like Persistent Identificatory Links, Public Immutability, and Ambiguity of Control and Processing that complicate compliance with data protection frameworks such as Nigerian Data Protection Regulation (NDPR), GDPR, and Personal Information Protection Law (PIPL). Biometric data are unique, permanent, and irrevocable identifiers. They are also associated with inherent privacy risks, distinct irrevocability and lifetime identity theft, unauthorised surveillance and function creep, and cross-database linkage.(Tran et al. 2021)

Figure 1.0 Emerging Technologies




## 2.1 OVERVIEW OF DATA PROTECTION REGULATION

Data protection regulations are a set of legal rules governing the collection, processing, use, archival and disposal/deletion of users' personal data with the aim of safeguarding individuals' right to privacy. These regulation creates a legal framework to be followed by organisations (data collectors and processors) and Accord rights to the individual (data subject) whose data is processed (Ekpo et al. 2024). Nigeria is regarded as the most populous country in Africa with a robust digital economy that supports thriving fintech,

digital commerce, and communication technology, which operate with user data. Nonetheless, this development accelerated issues surfacing data compromise, identity fraud and cybercrime, provoking inquiry on how resilience can be achieved through legal and regulatory framework (Stephanie Nma Modilim et al. 2024). First established was the Nigeria Cybercrime Act 2015, as the foundational legal framework, which focuses on combating the intensifying menace of cybercrime with the main function as retributive and deterrent, conferring necessary legal, regulatory and institutional structure for the prohibition, prevention and punishment of cybercrime in Nigeria (Eboibi 2017). Subsequently, in 2019, the first comprehensive and dedicated data protection regulation, the NDPR, was enacted by the National Information Technology Development Agency (NITDA), which aligns Nigeria closer to global standards like GDPR, NDPR focuses on protecting user data in this emerging technology era, the likes of Big Data, IoT, AI, and XR (Aloamaka 2023b). Furthermore, the framework advocates the systematic integration of privacy by design (PbD) in all data processing operations with technical and procedural measures, including Data Protection Impact Assessments (DPIAs), pseudonymisation, encryption, and access control. Conclusively, the framework is directed towards mandatory periodic compliance review, warranting that data controllers are adherent to compliance ("NDPR-Implementation-Framework," n.d.).

### 2.1.1 Regulatory Framework: The Nigeria Data Protection Act (NDPA) 2023 and Global Alignment

The NDPA of 2023 serves as the foundational body that ensures compliance with challenges inherent in all the emerging technologies in Nigeria. The Act is widely esteemed as a major legislative accomplishment: "The NDPA 2023 marks a pivotal advancement in Nigeria's regulatory framework for data protection" (Aloamaka 2025). This government signals a broad national purpose to align with global systems.

The NDPA provides the critical legal framework for data processing, as the article vividly examines the Act, featuring its alignment with the GDPR of the European Union and its effectiveness for Nigeria (Aloamaka 2025). This alignment with GDPR elevates Nigeria's standards for privacy rights and data protection of individuals, controls regulations across all technology applications, from AI to IoT. Moreover, the NDPA is the key policy that

leverages managing the opportunities and risks associated with every emerging technology application.

### 2.1.2 Cybercrime Act (2015, amended)

The Cybercrime Act (2015, amended) of Nigeria is the main primary law for combating cyber-related crimes, which establishes a legal act to detect, prevent, investigate, and prosecute cyber-related offences such as hacking (unauthorised access), identity theft, phishing, cyber-stalking, online fraud, and attacks on critical national infrastructure. The Act also enforces service providers to retain traffic and subscriber data for law enforcement purposes, and it empowers courts to issue orders for the interception of communications. This Act emphasises criminalising unauthorised access and misuse of devices and information; it aims to protect the data integrity, confidentiality, and availability of information systems within Nigeria.

The Act also prescribes penalties ranging from fines of millions of Naira to imprisonment (up to life sentences in severe cases, such as cyber-terrorism). The Act has been amended to address evolving crime, such as emerging threats, and expand enforcement powers as digital technology evolves. Although it primarily focuses on punishing cyber-related misconduct after it occurs, it is considered a pivotal step toward strengthening Nigeria's cybersecurity landscape and safeguarding individual, public, and private sectors from the growing risks of cybercrime

Table 1.0 Comparison of GDPR (EU), NDPA (Nigeria) and DPDP (India)

| Feature | GDPR (EU) 2016 | NDPA (Nigeria) 2023 | DPDP (India) 2023 |
|---|---|---|---|
| **Jurisdiction** | European Union (EU) and EEA; applies globally to the data of EU citizens | Nigeria applies to citizens/residents and foreign entities offering goods/services | India applies to digital data within India and foreign entities providing goods/services |
| **Objectives** | Focus on all Personal Data (digital or non-digital) | Focus on personal data (digital or non-digital) | Focus only on digital personal data. |

| | | | |
|---|---|---|---|
| **Scope** | Individual control over data, data minimisation, consent, right to be forgotten | Protects the privacy of individuals, regulates the processing of personal data, ensure lawful handling of data | Consent-based framework, cross-border transfer, data fiduciary obligations |
| **Key Principles** | Lawfulness, Fairness & Transparency; Purpose Limitation; Data Minimization; Integrity & Confidentiality; Accountability | Lawfulness, Fairness, Purpose Limitation, Data Minimisation, Integrity & Confidentiality, Accountability | Lawfulness, Purpose Limitation, Data Minimisation, Security Safeguards, Rights of Data Principals |
| **Consent** | Unambiguous, informed, explicit consent required | Unambiguous, informed consent is required | Explicit consent required; withdrawal allowed; stricter for children's data |
| **Right to Erasure (Deletion)** | Right to erasure ('Right to be Forgotten') under certain conditions | Right to request deletion of personal data under certain conditions | Recognises the right to correction and erasure of personal data |
| **Penalties** | Penalties start from reprimands or a small amount, up to €20 million or 4% of annual global turnover | Penalties start from ₦2 million up to ₦10 million for individuals or 2% of annual revenue for organisations | Penalty start from ₹50 crore to ₹250 crore (~USD 30M) |
| **Breach Notification** | Notify the authority within 72 hours; affected individuals without undue delay | Notify the Nigeria Data Protection Commission (NDPC) and affected individuals | Notify the Data Protection Board of India; rules evolving |
| **Future Outlook** | Continuous updates to address AI and emerging tech | Strengthening enforcement, new subsidiary regulations expected | Implementation rules, Data Protection Board functioning, and cross-border mechanisms expected by 2024–2025 |

### 2.1.3 Artificial Intelligence (AI) Act EU and Cybercrime Act (2015, amended 2024)

The table below compares the AI Act 2024 EU with the Nigerian Cybercrimes (Prohibition, Prevention, etc.) Act (2015, amended 2024), focusing on their scope, emerging technology implications, and penalties. This will help us to understand the gap and the need for a similar Act in Nigeria.

Table 2.0 Comparison of AI Act EU and Cybercrime Act (2015, amended 2024)

| Feature | EU AI Act (2024) | Nigeria Cybercrimes Act (2015, amended 2024) |
|---|---|---|
| **Objective** | Regulates the development, integration, and use of AI systems in the EU based on risk, ensuring safety, transparency, and respect for rights. | Criminalises and prevents cybercrimes such as unauthorised access, data misuse, fraud, and protects national security/economic interests. |
| **Scope** | Applies to AI systems (including biometric, generative AI, etc). Covers providers, deployers, importers, and distributors affecting EU citizens. | Applies to all computer systems, networks, and data. Covers individuals and organisations in Nigeria and abroad whose acts affect Nigeria. |
| **Regulatory Approach** | Risk-based classification: prohibited, high-risk, limited-risk, minimal-risk. High-risk AI must meet strict compliance. Prohibited AI is banned outright. | Criminalisation approach: defines specific offences (unauthorised access, identity theft, data misuse, fraud). Does not classify by risk but prohibits unlawful activities outright. |
| **Emerging Technologies Focus** | Explicitly addresses AI & emerging tech (Large Language Models (LLMs), generative AI, biometric surveillance, emotion recognition). Creates special | Indirectly covers emerging tech via cybercrimes (data breaches, phishing, identity theft, hacking of AI systems). No direct mention of AI, but provisions can apply to AI misuse. |

| | | |
|---|---|---|
| | obligations for General Purpose AI (GPAI). | |
| **Transparency & Data Requirements** | Mandates data quality, bias checks, documentation, human oversight, and transparency for high-risk and GPAI systems. Providers must supply technical documentation. | Requires data protection and reporting of breaches by service providers. Does not impose transparency requirements on algorithms but criminalises the misuse of data and unauthorised access. |
| **Prohibited Practices** | Bans certain AI uses outright: social scoring, real-time remote biometric ID in public (limited exceptions), and manipulative or exploitative AI. | Bans cybercrime activities such as unauthorised access, data interception, misuse, and sale of personal/financial data. No explicit prohibition on AI use. |
| **Penalties (Severe)** | Prohibited AI: up to €35 million or 7% of global turnover.<br>High-risk AI non-compliance: up to €15 million or 3% of turnover.<br>Misleading information: up to €7.5 million or 1% of turnover. | Unauthorised access: up to 2 years imprisonment or ₦5 million fine.<br>Data interception: up to 5 years imprisonment or ₦10 million fine.<br>Fraud/data misuse: up to 7 years imprisonment.<br>Organisations may face liability and sanctions for breaches. |
| **SMEs / Startups Consideration** | Provisions to ease compliance burden for SMEs but still binding. | No specific SME-friendly provisions; the law applies uniformly. |

## 3.0 EMERGING TECHNOLOGIES AND APPLICATIONS

The Nigerian industrial ecosystem is rapidly embracing these two technologies, AI and Big Data Analytics (BDA), with the intention to create a suitable infrastructure where emerging technologies are set to reformulate industries, boost the economic growth of Nigeria, and enhance citizens' lives. This evolution reaches numerous sectors in the industries, ranging from education, healthcare, agriculture, and other governmental branches. In the finance

and e-commerce sphere, the emergence of technological stalwarts like Flutterwave and Paystack presents how Nigerian startups can show their intellect globally while nurturing innovation and economic growth (Agbeyangi et al. 2024). The investment in IT, especially in the mobile platforms, has helped the financial inclusion for those living in difficult-to-reach areas, which enables them to significantly engage in saving, investing, and enhance the country's economy (Agbeyangi et al. 2024). Moreover, the adoption of AI at the same time raises challenges for data protection in bodies like transit, banking, healthcare, marketing, and e-commerce, where lots of data is collected as record-keeping (CIPESA 2024).

The application of BDA and AI provides a significantly useful system within the Nigerian logistics and transportation commercial enterprise. These technologies are rapidly changing the supply chain sustainability by improving efficiency and reducing environmental impact (Ojadi et al. 2024). In the healthcare sector, big data analytics is viewed as having the potential to transform healthcare by improving the quality of patient care, reducing medical errors, and decreasing the costs of healthcare delivery in Nigeria. This ability stems from BDA's capacity to detect trends, patterns, and relationships in patient data that may be overlooked by conventional approaches (V. et al. 2017).

### A. Internet of Things (IoT) in Smart Cities, Healthcare, and Agriculture

The Internet of Things (IoT) is an important component of the fourth industrial revolution (4IR), which is also Industry 4.0, a development where many authors come to the conclusion that it is here to stay, which is fast bridging the line between physical, digital, and online systems (Ukwandu et al., n.d.). In Nigeria, the potential of IoT covers several critical bodies with potential applications ranging across Smart environment, Smart cities, Smart Home, Smart Transport, Smart health, Smart farming, etc. The general impact of IoT technology is implemented in the realm of urban management and the public environment. For example, Smart City technology will help Nigeria improve traffic management, reduce crime and pollution, save energy, improve waste management and also improve the quality of life of its citizens (Ayobami Joshua 2020). Also, the introduction of Smart Grid technology can help regulate the power system of Nigeria,

which will enable Nigeria to achieve better electricity metering, monitor the efficiency of the electricity, billing and dispersion to end users or citizens (Ayobami Joshua 2020).

In the Healthcare sector, IoT is set to play a completely new function which have the ability to transform the healthcare system of Nigeria by enhancing the quality of patient care, minimising medical errors, and lowering the healthcare delivery cost. The core functionality lies in enabling real-time observation of patients' health status, remote consultation by doctors or nurses, and early detection of diseases. This accomplishment is achieved via the connected hardware devices that are embedded on medical machines, such as wearable sensors, smart beds, and remote monitoring systems, which show the patient's vital data on a screen, activity levels, and medication support (V. et al. 2017).

Furthermore, the implementation of IoT in the agricultural sector is a vital step to achieve higher productivity and ensure food security across Nigeria. This methodology works hand in hand with hardware devices connected to the agricultural tool, connecting the IoT-enabled devices to enhance crop yield processes and growth conditions while reducing financial cost and complexity of the farming process. In the Nigerian context, the implementation of smart technologies in agriculture is important because it plays a significant role in assisting farmers in low- and middle-income countries (LMICS) to increase their productivity and adapt to disasters (Salahudeen et al. 2022). The approach entails data acquisition directly from the field to the cloud, where sensors are installed in farmlands to monitor the weather conditions, soil quality, water levels, moisture and humidity, and crop growth progress by the farmers (Khan and Ullah 2024).

### B. Blockchain for Secure Transactions and Digital Identity

The idea of implementing blockchain technology in Nigeria is primarily focused on the need for embracing or modernising the industrial sectors, an advanced, secure system for users, and a privacy-preserving environment for National Identity Management, which leads to research specifically addressing this technology on hand as a necessary advancement (Agu and Hammawa 2019). Also, the development of the digital era, deep acknowledgement of the prospects of rising technologies, where the Nigerian researchers look into the importance of AI, blockchain, and the IoT by portraying the extraordinary

opportunities in the fields (Agbeyangi et al. 2024). Moreover, the usage of blockchain technology has had an essential impact on governance bodies in recent years, offering both possibilities and objections for many industries globally (Wu 2024).

Managing privacy and compliance with the data under legal laws is a core challenge for widespread blockchain technology adoption. The NDPA Act 2023 sets a crucial illustration for data protection in Nigeria, and its provisions have cultivated implications for blockchain technology, where some organisations embraced the system like NITDA, Stakeholders in Blockchain Association of Nigeria (SIBAN), and Blockchain Experts Association of Nigeria (BNUG) (Morenike et al., n.d.). This conflict of blockchain nature due to transparency and decentralised storage system intersects with data confidentiality. The best practice engineering approach is compulsory to formulate the solution between a shared record and the data subject's rights. Consequently, the result identifies the significance of blending data protection measures from the commencement of blockchain project development to ensure compliance with the NDPA and defend the confidentiality of private data (Morenike et al., n.d.).The main inherent attribute of transparency in the supply chain is what enables secure transactions and digital traceability, thereby rating the technology's usage in creating testable and safe logistics infrastructure (Ojadi et al. 2024).

### C. Biometrics Trust in the Public Sector and Banks

Nigeria's adoption of biometric technology has primarily been driven by the need for secure, reliable identity verification, which is encapsulated in the National Identification Number (NIN) managed by the National Identity Management Commission (NIMC) and Bank Verification Number (BVN) in the financial sector. The essential gain is seen as offering a useful asset over traditional token numbers and a password-based authentication system. The rationale behind this massive public sector and banking rollout is that the use of information and communication technology (ICT) is a requirement for authorities to fulfil their non-negotiable roles. Generally, the data analysis in the study revealed that ICT usage will enhance NIMC biometric activities (Olumide et al. 2023). In the process of enrolling all people in biometrics, bureaucratic competition has also played an important role, as demonstrated by historical reports about the CBN and NIMC's war over control of

the BVN program, highlighting the fragmented approach to national data systems regardless of the common inherent technology.

The biometric system provides an adequate impact of minimising fraudulent activity and ensuring unique identity in public and private sectors and introduces a unique and amplified privacy and security situation that impacts public trust. Given the centralisation of these sensitive, irreplaceable biological identifiers, the government and service providers have a non-negotiable obligation to uphold data integrity and privacy of their citizens (Olumide et al. 2023).

## 4.0 COMPLIANCE AND PRIVACY IMPLICATIONS IN EMERGING TECHNOLOGIES

Organisational operations are now advancing due to the trend in emerging technologies, which enhance efficiency, accuracy, transparency, and innovative solutions. For our privacy to be protected, addressing privacy is a significant concern that safeguards the use of our data without reputational, legal, and ethical damage. Nigeria, as one of the largest Internet users, the NDPR served as a guide for data usage in compliance with the ethical use of data. Likewise, the GDPR is a global regulation established by the EU to ensure compliance with privacy regulations. Agencies and organisations must work with such privacy in providing confidentiality, integrity, and transparency in safeguarding individual data (Olayanju Jayeola 2025).

### A. AI Lack of Explainability, Bias, and Discrimination

Systems using AI rely on large datasets for automating decisions and predictions; if these datasets are found to be incomplete, unrepresentative, or biased. In that case, the system's outcome can be discriminatory, which directly impacts law enforcement, the healthcare system, financial services, the government, or the educational system (Zhao et al. 2020). AI "Black boxes" usually decide without using clear reasoning. Organisations and agencies under the GDPR and NDPR are required to ensure that decision-making is transparent, ethical, and fair, and that the individual clearly understands the process by which the data is being used. To ensure these happened:

A. Anonymisation and minimising the data usage lowers the risk of sensitive information being disclosed
B. Make the decision interpretable by using Explainable AI frameworks (e.g., LIME or SHAP)
C. Evaluating the algorithm to identify the potential bias or incompleteness for sensitive information
D. Regular checkup for adherence to the regulators for ethical and legal use of individual rights.

Taking these measures will ensure accountability, transparency, and minimise bias in decision-making, thereby building trust expected with emerging technologies that are legally compliant (Zhao et al. 2020).

### B. Differential Privacy and Big Data

By collecting a large-scale personal dataset, organisations can equip themselves to analyse big data and uncover valuable insights. This enables businesses to incorporate more intelligent processes, but the violation of privacy increases, including the breach of individuals' data and profiling (Chamikara et al. 2020a). To erase the possibility of such an occurrence, the following compliance strategies must be observed:

i. Using PIAs in evaluating data risk and any harmful potential in the dataset
ii. Compliance with the policies provided by the data governance for using the data, which clearly indicates the purpose of collecting it and the benefits of it.
iii. Recent privacy techniques introduce the use of noise in datasets, which reduces the risk of identifying individual privacy and improves efficiency, audibility, and transparency by integrating blockchain technology into tracking the usage of differential privacy (Chamikara et al. 2020b).

### C. IoT Security Devices and Consent Management

Devices such as smart watches, home connected systems, self-driving cars, and smart meters, which use the Internet of Things (IoT), continuously produce personal data, real-time surveillance, and illegal access. To mitigate the occurrence of such data, the organisations must ensure:

i. They provide a user-friendly dashboard to constantly monitor, permit, delete, revoke, and provide access to their data.
ii. Integrating design with privacy principles from the initial development stage.
iii. Provide encryption mechanisms and security protocols to constantly allow users to identify any kind of penetration and vulnerability early

These strategies mitigate the risks associated with breaching individuals' data rights and standardise processes in compliance with national and international privacy regulations (Jonah 2024).

### D. Blockchain for Consent and Data Integrity

Blockchain technology ensures integrity, making the ledgers unchangeable and preventing regulatory bodies from erasing or rectifying data that creates conflicts with privacy rights. Such services provide the best practice by maintaining the integrity of sensitive information, making the information encrypted throughout the processes on the chain, and lastly, consent management implementation for tracking and enabling user permission (smart contract). These ensure the data remains valid throughout, which, combined, build trust by making the user and their data fully protected and invisible to alteration.

The right to erasure in blockchain ledger conflicts with GDPR or NDPA, which requires implementation of a hybrid strategy to preserve the integrity of the data while on-chain and allow modification of the off-chain to ensure the data is not tampered with on the ledger (Lai et al. 2024).

### E. Biometrics: Privacy and Security

Obtaining information from biometrics, such as iris scans, facial recognition, and fingerprints, is described as a unique and sensitive means of obtaining an individual's biometric record. Obtaining access to such information will provide direct and permanent surveillance on an individual, which can risk the illegal use of an individual's rights. To avoid such, an organisation should implement an access control mechanism and encryption mechanism for the database, provide consent to the user on the collection and use of the data, and audit unauthorised and misuse of the data to avoid unnecessary use. Such

implementation will provide complete control over what, where, and how the information is being used accordingly.

To utilise biometrics in Nigeria, risks include illegal surveillance, data tampering, and unnecessary revocation procedures, as the system is employed by various agencies within the country, such as the Independent National Electoral Commission (INEC), the National Identity Management System, the banking system, and Ministries. To mitigate such risks, a decentralised biometric system was proposed, which utilises zero-knowledge proofs to protect users by providing only permits for verification, thereby avoiding the disclosure of raw biometric data (Chamikara et al. 2020a).

### F. Compliance Framework for Privacy-by-Design

Features for protection must be implemented at the earliest stage of system design, which is the reason for privacy-by-design. The core fundamentals include: regular auditing to ensure the system complies with regulatory standards, Privacy activities supervision by setting up a Data Protection Officer (DPO), and integration of technical and organisational protection from design to implementation (Olayanju Jayeola 2025). Adhering to these policies will strengthen the system and foster trust in the protection and monitoring of privacy.

Table 3.0 Comparison between Emerging Technologies

| **Technology/Area** | **Risks / Issues** | **Compliance & Mitigation Strategies** | **Regulatory Implications (GDPR/NDPR/Global)** |
|---|---|---|---|
| **AI & Algorithmic Transparency** | Biased or incomplete datasets, Black-box decision making, Discrimination in healthcare, finance, education, etc. | Anonymisation & data minimisation, Explainable AI (e.g., LIME, SHAP), Bias evaluation & audits, Regular compliance checks | GDPR & NDPR require fairness, transparency, and explainability in automated decisions. |

| | | | |
|---|---|---|---|
| **Differential Privacy & Big Data** | Risk of data breaches, Profiling & misuse of personal datasets, Loss of confidentiality | Privacy Impact Assessments (PIAs), Data governance & clear purpose policies, Noise addition in datasets. | Compliance with NDPR & GDPR mandates lawful, fair, and limited data usage |
| **IoT Devices & Consent Management** | Continuous personal data generation, Unauthorised surveillance & access, Device vulnerabilities | User dashboards for consent & control, Privacy-by-design in development, Strong encryption & early vulnerability detection | GDPR/NDPR require explicit user consent & accountability for IoT data |
| **Blockchain for Consent & Data Integrity** | Immutable ledgers conflict with the right to erasure. Risk of non-compliance with rectification laws | Encryption & integrity mechanisms, Smart contracts for consent management, Hybrid approach (on-chain integrity + off-chain modification) | GDPR: Right to erasure/rectification, NDPR: Requires hybrid compliance for blockchain systems |
| **Biometrics: Privacy & Security** | Permanent surveillance risks Data tampering & unauthorised access Revocation challenges | Access control & encryption, User consent mechanisms, Auditing unauthorised use, Zero-knowledge proofs for verification | GDPR/NDPR treat biometrics as "sensitive data" requiring strict protection |

### G. Incoherence of Jurisdiction and Cross-Border Flow of Data

Bypassing data outside Nigeria by NDPR/NDPA will be complex due to policy differences between the affected nations. Adhering to such services, an International standard needs to be established that defines the corporate rules to maintain integrity and accountability. This

will foster a strong relationship, promote honesty, and facilitate the transfer of protected and sensitive information across borders (“Africa AI - Privacy Report,” n.d.).

### H. Challenges and Barriers to Nations' Development

The application of emerging technologies in Nigeria is fundamentally hampered by persisting infrastructure and capacity constraints, as well as novel security and ethical concerns. One of the main obstacles is the absence of universal access, which calls for the urgency of achieving digital inclusivity, bridging the urban-rural gap, and reducing the technological divide (Agbeyangi et al. 2024). Technical hindrance further compounds this difficulty, as the IoT, irrespective of its vast potential, is currently constrained by the absence of reliable security measures that ensure protection of data (Ayobami Joshua 2020). Furthermore, the human resources needed to support this technological revolution are rapidly standing out. For instance, the adoption of modern paradigms such as ARCHITECTURE 5.0 in the construction sector presents significant obstacles because of skill gaps and inadequate training and educational awareness on this technology (T. A. 2024). In the case of a biometric system, once data has been collected, it is a permanent, non-revocable identification machine, and because of that, a security breach of data represents an immutable threat to the user's long-term security, raising major privacy and security concerns.

The nation is more vulnerable to complicated security threats because of these deficiencies in technical and human capital. An environment of complex cyber and physical systems that are inevitably vulnerable to various types of sophisticated Cyber-Attacks has been produced by the Fourth Industrial Revolution (4IR), which has been fast bridging the line between physical, digital, and natural systems" (Ukwandu et al., n.d.). Continual policy and capacity-building initiatives are needed to address this based on the ambitious objective of the 3 Million Tech Talents (3MTT) program across Nigeria, which continues proactively to develop a skilled labour force (Agbeyangi et al. 2024). Therefore, achieving an inclusive and dependable digital future still depends on addressing the triple problem of infrastructure constraints, cybersecurity vulnerabilities, and the development of skills.

## 5.0 CONCLUSION AND RECOMMENDATIONS

Emerging technologies such as AI, Big Data, IoT, Blockchain, Cloud Computing drive an innovation but also trigger significant risks to regulatory compliance and data privacy. In Nigerian context, the key issues lies in the weak enforcement of the existing frameworks NDPA and NDPR, and the lack of a comprehensive polices like an AI Act.

To address some of these challenges, stronger enforcement of data protection laws needs to be deployed, enhanced strong collaborations among regulators, bring industry stakeholders and policymakers on board, as well as improve public awareness and capacity building in this context. Regular security assessments for high-risk technologies such as AI and IOT should be mandated to uphold data CIA.

By enabling this embedding policy and compliance framework design, organizations can strongly build user trust, protect and prevent data breaches, and drive sustainable digital growth exponentially. Finally, developing Nigeria-specific policy frameworks inspired by models such as the EU's AI Act, will strengthen privacy standards and ensure reliable, responsible innovation in the digital economy

## REFERENCES


1. "Africa AI - Privacy Report." n.d.

2. Agbeyangi, A. O., A. S. Makinde, and I. A. Odun-Ayo. 2024. *Nigeria's ICT and Economic Sustainability in the Digital Age*. Chrisland University, Abeokuta; Edo State University, Uzairue. https://arxiv.org/pdf/2401.03996.pdf.

3. Agu, Edward Onyebueke, and Mohammed Hammawa. 2019. *Development of a National Identity Management System Using Blockchain Technology*. 12 (4).

4. Ajayi, Olumide. 2025. "Data Privacy and Regulatory Compliance: A Call for a Centralized Regulatory Framework." *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.5044945.

5. Alkaeed, Mahdi, Adnan Qayyum, and Junaid Qadir. 2024. "Privacy Preservation in Artificial Intelligence and Extended Reality (AI-XR) Metaverses: A Survey."

*Journal of Network and Computer Applications* 231 (November): 103989. https://doi.org/10.1016/j.jnca.2024.103989.

6. Aloamaka, P. C. Aloamaka. 2023a. “DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA: LESSONS FROM OTHER JURISDICTIONS.” *UCC Law Journal* 3 (1): 281–321. https://doi.org/10.47963/ucclj.v3i1.1259.

7. Aloamaka, P. C. Aloamaka. 2023b. “DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA: LESSONS FROM OTHER JURISDICTIONS.” *UCC Law Journal* 3 (1): 281–321. https://doi.org/10.47963/ucclj.v3i1.1259.

8. Aloamaka, Patrick Chukwunonso Aloamaka. 2025. “A CRITICAL ANALYSIS OF THE NIGERIA DATA PROTECTION ACT 2023: ELEVATING STANDARDS TO GLOBAL NORMS.” *UCC Law Journal* 4 (2): 242–63. https://doi.org/10.47963/ucclj.v4i2.1724.

9. Ayobami Joshua, Ayeni. 2020. “Internet of Things (IoT): The Technology, Architecture and Applications – Prospects in Nigeria.” *Internet of Things and Cloud Computing* 8 (4): 41. https://doi.org/10.11648/j.iotcc.20200804.11.

10. Chamikara, M. A. P., P. Bertok, I. Khalil, D. Liu, and S. Camtepe. 2020a. “Privacy Preserving Face Recognition Utilising Differential Privacy.” *Computers & Security* 97 (October): 101951. https://doi.org/10.1016/j.cose.2020.101951.

11. Chamikara, M. A. P., P. Bertok, I. Khalil, D. Liu, and S. Camtepe. 2020b. “Privacy Preserving Face Recognition Utilising Differential Privacy.” *Computers & Security* 97 (October): 101951. https://doi.org/10.1016/j.cose.2020.101951.

12. CIPESA. 2024. *The Impact of Artificial Intelligence on Data Protection and Privacy: A Walk-through Rights of a Data Subject in Africa*. Policy Brief / Report. Collaboration on International ICT Policy for East and Southern Africa (CIPESA). https://cipesa.org/wp-content/files/briefs/The_Impact_of_Artificial_Intelligence_on_Data_Protection_and_Privacy_-_Brief.pdf.

13. Dhirani, Lubna Luxmi, Noorain Mukhtiar, Bhawani Shankar Chowdhry, and Thomas Newe. 2023a. “Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review.” *Sensors* 23 (3): 1151. https://doi.org/10.3390/s23031151.

14. Dhirani, Lubna Luxmi, Noorain Mukhtiar, Bhawani Shankar Chowdhry, and Thomas Newe. 2023b. “Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review.” *Sensors* 23 (3): 1151. https://doi.org/10.3390/s23031151.

15. Eboibi, Felix E. 2017. “A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015.” *Computer Law & Security Review* 33 (5): 700–717. https://doi.org/10.1016/j.clsr.2017.03.020.

16. Ekpo, Otuekong, Abasifiok Okokon, and Monday Akpakpan. 2024. “Data Protection in the Digital Age: A Comparative Analysis of Nigeria’s NDPA and the EU’s GDPR.” *Proceedings of the 13th International Conference on Information & Communication Technologies and Development*, December 9, 48–56. https://doi.org/10.1145/3700794.3700799.

17. Jonah, Kings. 2024. “A Comparative Analysis of the Nigerian Data Protection Act 2023, and the EU General Data Protection Regulations Applicable in the United Kingdom.” *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.4680532.

18. Khan, Muhammad Kabir, and Adnan Ullah. 2024. “Implication of IoT and Its Impact on Library Services: An Overview.” *Inverge Journal of Social Sciences (IJSS)* 3 (2): 10.

19. Lai, Junhao, Taotao Wang, Shengli Zhang, Qing Yang, and Soung Chang Liew. 2024. “BioZero: An Efficient and Privacy-Preserving Decentralized Biometric Authentication Protocol on Open Blockchain.” arXiv:2409.17509. Preprint, arXiv, September 26. https://doi.org/10.48550/arXiv.2409.17509.

20. Morenike, Elesho Oluwabukolami, Grace Ihinosen Akhihiero, Okhiai Elizabeth Blessing, et al. n.d. *BLOCKCHAIN AND DATA PROTECTION BY DESIGN: AN EXAMINATION OF THE NDPA'S PROVISIONS AND BEST PRACTICES.*

21. "NDPR-Implementation-Framework." n.d.

22. Ojadi, Jessica Obianuju, Chinekwu Somtochukwu Odionu, Ekene Cynthia Onukwulu, and Olumide Akindele Owulade. 2024. "Big Data Analytics and AI for Optimizing Supply Chain Sustainability and Reducing Greenhouse Gas Emissions in Logistics and Transportation." *International Journal of Multidisciplinary Research and Growth Evaluation.* 5 (1): 1536–48. https://doi.org/10.54660/.IJMRGE.2024.5.1.1536-1548.

23. Olayanju Jayeola, Abdulhakeem. 2025. "Artificial Intelligence And The Law: An Examination Of The Functionality Of Data Protection Laws In Nigeria." Preprint, SSRN. https://doi.org/10.2139/ssrn.5017252.

24. Olumide, George Olu, Tolulope Isaac Olatunji, and Okechukwu Nwachukwu. 2023. "Biometric Information Management in Nigeria: A Case of National Identity Management Commission." *Information Impact: Journal of Information and Knowledge Management* 14 (3): 117–27.

25. Pinto, George P., Praveen Kumar Donta, Schahram Dustdar, and Cássio Prazeres. 2024. "A Systematic Review on Privacy-Aware IoT Personal Data Stores." *Sensors* 24 (7): 2197. https://doi.org/10.3390/s24072197.

26. Salahudeen, Mudathir Muhammad, Muhammad Auwal Mukhtar, and Saadu Salihu Abubakar. 2022. *Mobile Technology: A Panacea to Food Insecurity in Nigeria*.

27. Stephanie Nma Modilim, Iyanuoluwa Bolarinwa, Motunrayo Tolani Omidiora, and Obah Tawo. 2024. *Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment.* Vol. 7 Iss 6; 2481 (January). https://doi.org/10.10000/IJLMH.119827.

28. T. A., Suleman. 2024. “Architecture 5.0: Opportunities and Challenges in the Nigerian Construction Industry.” *British Journal of Computer, Networking and Information Technology* 7 (4): 118–32. https://doi.org/10.52589/BJCNIT-HUWAI7DU.

29. Tran, Hong-Yen, and Jiankun Hu. 2019. “Privacy-Preserving Big Data Analytics a Comprehensive Survey.” *Journal of Parallel and Distributed Computing* 134 (December): 207–18. https://doi.org/10.1016/j.jpdc.2019.08.007.

30. Tran, Quang Nhat, Benjamin P. Turnbull, and Jiankun Hu. 2021. “Biometrics and Privacy-Preservation: How Do They Evolve?” *IEEE Open Journal of the Computer Society* 2: 179–91. https://doi.org/10.1109/OJCS.2021.3068385.

31. Ukwandu, Elochukwu A, Ephraim N C Okafor, Charles Ikerionwu, Comfort Olebara, and Celestine Ugwu. n.d. *Cyber-Security in the Emerging World of ’Smart Everything’*.

32. V., Oluigbo Ikenna, Department of Information Management Technology, Federal University of Technology Owerri, Imo State, Nigeria, Nwokonkwo Obi C., et al. 2017. “Revolutionising the Healthcare Industry in Nigeria The Role of Internet of Things and Big Data Analytics.” *International Journal of Scientific Research in Computer Science and Engineering* 5 (6): 1–12. https://doi.org/10.26438/ijsrcse/v5i6.112.

33. Wu, Tong. 2024. “Exploring of the Integration of Emerging Technologies and Corporate Governance.” *Advances in Economics, Management and Political Sciences* 87 (1): 90–96. https://doi.org/10.54254/2754-1169/87/20241021.

34. Yuan, Zhang Si, and Manmeet Mahinderjit Singh. n.d. *Privacy Risks in Health Big Data: A Systematic Literature Review*.

35. Zafar, Ammar. 2025. “Reconciling Blockchain Technology and Data Protection Laws: Regulatory Challenges, Technical Solutions, and Practical Pathways.” *Journal of Cybersecurity* 11 (1): tyaf002. https://doi.org/10.1093/cybsec/tyaf002.

36. Zhao, Yang, Jun Zhao, Jiawen Kang, Zehang Zhang, Dusit Niyato, and Shuyu Shi. 2020. “A Blockchain-Based Approach for Saving and Tracking Differential-Privacy Cost.” arXiv:2001.09259. Preprint, arXiv, December 22. https://doi.org/10.48550/arXiv.2001.09259.